

CLAIMS

WHAT IS CLAIMED IS:

1. A method of securely accessing data in a personal computer, the method comprising:  
reading a secret from a first location;  
5 securing the secret in a secure location different from the first location; and  
retrieving at least a portion of the data stored in the first location using the secret.

2. The method of claim 1, wherein the first location comprises a memory;  
wherein reading the secret from the first location comprises reading the secret from the  
10 memory;  
wherein securing the secret in the secure location different from the first location comprises  
securing the secret in the secure location different from the memory; and  
wherein retrieving at least the portion of the data stored in the first location using the secret  
comprises retrieving at least the portion of the data stored in the memory using the  
15 secret.

3. The method of claim 2, wherein the memory is a read-only memory (ROM);  
wherein reading a secret from the memory comprises reading the secret from the ROM;  
wherein securing the secret in a secure location different from the memory comprises  
20 securing the secret in the secure location different from the ROM; and  
wherein retrieving at least a portion of the data stored in the memory using the secret  
comprises retrieving at least the portion of the data stored in the ROM using the  
secret.

4. The method of claim 3, wherein the data comprises basic input-output system (BIOS) data and the ROM is a BIOS ROM configured to store the BIOS data;

wherein reading the secret from the ROM comprises reading the secret from the BIOS ROM;

wherein securing the secret in the secure location different from the ROM comprises securing

5 the secret in the secure location different from the BIOS ROM; and

wherein retrieving at least a portion of the data stored in the ROM using the secret comprises

retrieving at least a portion of the BIOS data stored in the BIOS ROM using the secret.

10 5. The method of claim 3, wherein reading the secret from the ROM comprises reading the secret from within the data stored within the ROM.

6. The method of claim 1, further comprising:

15 reading code from the first location, wherein the code is different from the secret and different from the data stored in the first location;

wherein retrieving at least a portion of the data stored in the first location using the secret comprises retrieving at least a portion of the data stored in the first location using the code and the secret.

20 7. The method of claim 6, wherein the first location comprises a memory;

wherein reading the secret from the first location comprises reading the secret from the memory;

wherein securing the secret in the secure location different from the first location comprises securing the secret in the secure location different from the memory;

wherein retrieving at least the portion of the data stored in the first location using the secret comprises retrieving at least the portion of the data stored in the memory using the secret;

wherein reading code from the first location comprises reading code from the memory wherein the code is different from the secret and different from the data stored in the memory; and

wherein retrieving at least the portion of the data stored in the first location using the code and the secret comprises retrieving at least a portion of the data stored in the memory using the code and the secret.

8. The method of claim 7, wherein reading the secret within the memory and reading code from the memory further comprises reading the secret from inside the code within the memory.

9. The method of claim 6, further comprising:  
unlocking a lock bit associated with the data stored in the first location prior to retrieving at least the portion of the data stored in the first location using the secret.

10. The method of claim 9, wherein the location comprises a memory;  
wherein reading the secret from the first location comprises reading the secret from the memory;  
wherein securing the secret in the secure location different from the first location comprises securing the secret in the secure location different from the memory;

wherein retrieving at least the portion of the data stored in the first location using the secret comprises retrieving at least the portion of the data stored in the memory using the secret;

wherein reading code from the first location comprises reading code from the memory

5 wherein the code is different from the secret and different from the data stored in the memory;

wherein retrieving at least the portion of the data stored in the first location using the code and the secret comprises retrieving at least a portion of the data stored in the memory using the code and the secret; and

10 wherein unlocking the lock bit associated with the data stored in the first location prior to retrieving at least the portion of the data stored in the first location using the secret comprises unlocking the lock bit associated with the data stored in the memory prior to retrieving at least the portion of the data stored in the memory using the secret.

15 11. The method of claim 9, further comprising:

processing the secret using the code;

wherein unlocking a lock bit associated with the data stored in the first location comprises unlocking the lock bit associated with the data stored in the first location in response to processing the secret using the code.

20 12. The method of claim 11, wherein the first location comprises a memory;

wherein reading the secret from the first location comprises reading the secret from the memory;

wherein securing the secret in the secure location different from the first location comprises  
securing the secret in the secure location different from the memory;

wherein retrieving at least the portion of the data stored in the first location using the secret  
comprises retrieving at least the portion of the data stored in the memory using the  
5 secret;

wherein reading code from the first location comprises reading code from the memory,  
wherein the code is different from the secret and different from the data stored in the  
memory;

wherein retrieving at least the portion of the data stored in the first location using the code  
and the secret comprises retrieving at least a portion of the data stored in the memory  
10 using the code and the secret;

wherein unlocking the lock bit associated with the data stored in the first location prior to  
retrieving at least the portion of the data stored in the first location using the secret  
comprises unlocking the lock bit associated with the data stored in the memory prior  
15 to retrieving at least the portion of the data stored in the memory using the secret; and

wherein unlocking the lock bit associated with the data stored in the first location comprises  
unlocking the lock bit associated with the data stored in the memory in response to  
processing the secret using the code.

20 13. The method of claim 1, further comprising:

unlocking a lock bit associated with data stored in the first location prior to retrieving at least  
the portion of the data stored in the first location using the secret.

14. The method of claim 13, wherein the first location comprises a memory;

wherein reading the secret from the first location comprises reading the secret from the  
25 memory;

wherein securing the secret in the secure location different from the first location comprises

securing the secret in the secure location different from the memory;

wherein retrieving at least the portion of the data stored in the first location using the secret

comprises retrieving at least the portion of the data stored in the memory using the

5 secret; and

wherein unlocking a lock bit associated with data stored in the first location prior to

retrieving at least the portion of the data stored in the first location using the secret

comprises unlocking a lock bit associated with data stored in the memory prior to

retrieving at least the portion of the data stored in the memory using the secret.

10 15. The method of claim 1, further comprising:

storing the secret within the first location securely;

storing data within the first location securely; and

storing code different from the secret and different from the data within the first location

15 securely.

16. The method of claim 15, wherein the first location comprises a memory;

wherein reading the secret from the first location comprises reading the secret from the  
memory;

20 wherein securing the secret in the secure location different from the first location comprises

securing the secret in the secure location different from the memory;

wherein retrieving at least the portion of the data stored in the first location using the secret

comprises retrieving at least the portion of the data stored in the memory using the

secret;

wherein storing the secret within the first location securely comprises storing the secret within the memory securely;

wherein storing data within the first location securely comprises storing data within the memory securely; and

- 5 wherein storing code different from the secret and different from the data within the first location securely comprises storing code different from the secret and different from the data within the memory securely

17. The method of claim 16, wherein the memory is a read-only memory (ROM);

- 10 wherein storing a secret within the memory comprises storing a secret within the ROM;

wherein storing data within the memory comprises storing data within the ROM;

wherein storing code different from the secret and different from the data within the memory comprises storing code different within secret and different from the data within the ROM;

- 15 wherein securing the secret in a secure location different from the memory comprises securing the secret in a secure location different from the ROM; and  
wherein retrieving at least a portion of the data from the memory using the secret comprises retrieving at least a portion of the data from the ROM using the secret.

- 20 18. The method of claim 17, wherein the data comprises basic input-output system (BIOS) data and the ROM is a BIOS ROM configured to store the BIOS data;  
wherein storing a secret within the ROM comprises storing a secret within the BIOS ROM;  
wherein storing data within the ROM comprises storing data within the BIOS ROM;

wherein storing code different within secret and different from the data within the ROM  
comprises storing code different within secret and different from the BIOS data within  
the BIOS ROM;

wherein securing the secret in a secure location different from the ROM comprises securing  
the secret in a secure location different from the BIOS ROM; and

wherein retrieving at least a portion of the data from the ROM using the secret comprises  
retrieving at least a portion of the BIOS data from the BIOS ROM using the secret.

19. The method of claim 16, wherein storing a secret within the memory and storing data  
within the memory comprises storing the secret inside the data within the memory.

20. The method of claim 16, wherein storing a secret within the memory and storing code  
different from the secret and different from the data within the memory comprises  
storing the secret inside the code within the memory.

21. The method of claim 16, further comprising:  
unlocking a lock bit associated with the data prior to retrieving at least the portion of the data  
from the memory using the secret.

22. The method of claim 21, further comprising:  
reading the code from the memory; and  
securing the code in a secure location different from the memory;  
wherein retrieving at least a portion of the data from the memory using the secret comprises  
retrieving at least a portion of the data from the memory using the code and the secret.



23. The method of claim 22, wherein reading the secret from the memory comprises reading the secret from the memory during a boot sequence; and wherein securing the secret in a secure location different from the memory comprises storing the secret in SMM memory space.

5

24. The method of claim 22, wherein retrieving at least a portion of the data from the memory using the code and the secret further comprises:

processing the code; and

transmitting at least an indication of the secret to the memory;

10

25. The method of claim 24, wherein retrieving at least a portion of the data from the memory using the code and the secret further comprises:

receiving a challenge from the memory; and

transmitting a response to the memory including at least an indication of the secret to the memory, in response to receiving the challenge.

15

26. The method of claim 1, further comprising:

reading the code from the first location; and

securing the code in a secure location different from the first location;

20 wherein retrieving at least a portion of the data from the first location using the secret comprises retrieving at least a portion of the data from the first location using the code and the secret.

27. The method of claim 26, wherein the first location comprises a memory;

wherein reading the secret from the first location comprises reading the secret from the memory;

wherein securing the secret in the secure location different from the first location comprises securing the secret in the secure location different from the memory;

- 5 wherein retrieving at least the portion of the data stored in the first location using the secret comprises retrieving at least the portion of the data stored in the memory using the secret;

wherein reading the code from the reading the code from the memory comprises reading the code from the memory;

- 10 wherein securing the code in a secure location different from the first location comprises securing the code in a secure location different from the memory; and

wherein retrieving at least a portion of the data from the first location using the secret further comprises retrieving at least a portion of the data from the memory using the code and the secret.

15

28. The method of claim 1, wherein reading the secret from the first location comprises reading the secret from the first location during a boot sequence; and  
wherein securing the secret in a secure location different from the first location comprises storing the secret in SMM memory space.

20

29. The method of claim 28, wherein the first location comprises a memory;  
wherein reading the secret from the first location comprises reading the secret from a memory;

wherein securing the secret in the secure location different from the first location comprises

25

securing the secret in the secure location different from the memory;

wherein retrieving at least the portion of the data stored in the first location using the secret comprises retrieving at least the portion of the data stored in the memory using the secret; and

wherein reading the secret from the memory further comprises reading the secret from the memory during a boot sequence.

30. The method of claim 1, further comprising:

providing a lock bit associated with the data that when set provides an indication that the data stored in the memory is secured.

31. The method of claim 30, wherein the first location comprises a memory;

wherein reading the secret from the first location comprises reading the secret from the memory;

wherein securing the secret in the secure location different from the first location comprises securing the secret in the secure location different from the memory;

wherein retrieving at least the portion of the data stored in the first location using the secret comprises retrieving at least the portion of the data stored in the memory using the secret; and

wherein providing the lock bit associated with the data that when set provides an indication that the data stored in the first location is secured comprises providing a lock bit associated with the data that when set provides an indication that the data stored in the memory is secured

32. A method of securing data in a personal computer system, the method comprising:

storing a secret within a first location; and

storing code different from the secret within the first location;

wherein the code is configured to provide access to data stored in the first location when processed in association with the secret.

5 33. The method of claim 32, wherein the first location comprises a memory;

wherein storing the secret within the first location comprises storing a secret within the memory;

wherein storing code different from the secret within the first location comprises storing code different from the secret within the memory; and

10 wherein the code is configured to provide access to data stored in the first location when processed in association with the secret further comprises the code being configured to provide access to data stored in the memory when processed in association with the secret.

15

34. The method of claim 33, wherein the memory is a read-only memory (ROM);

wherein storing a secret within the memory comprises storing a secret within the ROM; and

wherein storing code different from the secret within the memory comprises storing code different within secret within the ROM; and

20 wherein the code is configured to provide access to data stored in the ROM when processed in association with the secret.

35. The method of claim 34, wherein the data comprises basic input-output system (BIOS) data and the ROM is a BIOS ROM configured to store the BIOS data;

25 wherein storing a secret within the ROM comprises storing a secret within the BIOS ROM;

wherein storing code different within secret within the ROM comprises storing code different within secret within the BIOS ROM; and

wherein the code is configured to provide access to BIOS data stored in the BISO ROM when processed in association with the secret.

5

36. The method of claim 33, wherein storing a secret within the memory comprises storing the secret inside the data within the memory.

37. The method of claim 33, wherein storing a secret within the memory and storing code different from the secret within the memory comprises storing the secret inside the code within the memory.

38. The method of claim 33, further comprising:

providing a lock bit associated with the data stored in the memory that when set provides an indication that the data stored in the memory is secured.

39. A personal computer system, comprising:

a first location configured to store code, a secret, and data different from the secret and different from the code;

a master device operably coupled to the first location, wherein the master device is configured to read the secret from the first location and to store the secret in a secure location different from the first location, and wherein the master device is further configured to access the data stored in the first location using the secret.

40. The personal computer system of claim 39, wherein the first location comprises a memory.

41. The personal computer system of claim 40, wherein the memory comprises a read-  
5 only memory (ROM).

42. The personal computer system of claim 41, wherein the ROM comprises a basic input-output system (BIOS) ROM, and wherein the data comprise BIOS data.

43. The personal computer system of claim 41, wherein the master device is further  
10 configured to read the secret from within the data stored within the ROM.

44. The computer system of claim 41, wherein the master device is further configured to  
15 read the code from the memory; and wherein the master device is further configured to retrieve at least a portion of the data stored in the memory using the code and the secret.

45. The computer system of claim 39, further comprising:

a lock bit associated with the data stored in the first location; and

20 wherein the master device is further configured to unlock the lock bit associated with the data stored in the first location.

46. The personal computer system of claim 45, wherein the first location comprises a memory.

47. The computer system of claim 46, wherein the master device is further configured to process the secret using the code; and wherein the master device is further configured to unlock the lock bit associated with the data stored in the memory in response to processing the secret using the code.

5 48. The computer system of claim 47, wherein the master device is further configured to receive a challenge from the memory and to transmit a response to the memory including at least an indication of the secret to the memory, in response to receiving the challenge.

10 49. The computer system of claim 39, wherein the master device is further configured to read the secret from the first location during a boot sequence; and wherein the master device is further configured to store the secret in SMM memory space.

15 50. The computer system of claim 39, wherein the master device includes a microprocessor.

51. A personal computer system, comprising:

20 means for securely storing data;

means for reading a secret from the means for securely storing data;

means for securing the secret in a secure location different from the means for securely storing data; and

25 means for retrieving at least a portion of the data stored in the means for securely storing data using the secret.

52. The personal computer system of claim 51, further comprising:

means for reading code from the means for securely storing data, wherein the code is  
different from the secret and different from the data stored in the means for securely  
storing data;

wherein the means for retrieving at least a portion of the data stored in the means for securely  
storing data from the means for securely storing data using the secret comprises  
means for retrieving at least a portion of the data stored in the means for securely  
storing data using the code and the secret.

53. The personal computer system of claim 51, further comprising:

means for locking the means for securely storing data; and  
means for unlocking the means for locking.

54. The personal computer system of claim 51, further comprising:

means for processing the secret using the code.

55. A method of securely accessing data in a personal computer, the method comprising:

step for reading a secret from a first location;

step for securing the secret in a secure location different from the first location; and

step for retrieving at least a portion of the data stored in the first location using the secret.

56. The method of claim 55, further comprising:

step for reading code from the first location, wherein the code is different from the secret and  
different from the data stored in the first location;



wherein the step for retrieving at least the portion of the data stored in the first location using the secret comprises step for retrieving at least the portion of the data stored in the first location using the code and the secret.

5 57. The method of claim 55, further comprising:

step for unlocking a lock bit associated with the data stored in the first location prior to the step for retrieving at least the portion of the data stored in the first location using the secret.

10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28  
29  
30  
31  
32  
33  
34  
35  
36  
37  
38  
39  
40  
41  
42  
43  
44  
45  
46  
47  
48  
49  
50  
51  
52  
53  
54  
55  
56  
57  
58  
59  
60  
61  
62  
63  
64  
65  
66  
67  
68  
69  
70  
71  
72  
73  
74  
75  
76  
77  
78  
79  
80  
81  
82  
83  
84  
85  
86  
87  
88  
89  
90  
91  
92  
93  
94  
95  
96  
97  
98  
99  
100  
101  
102  
103  
104  
105  
106  
107  
108  
109  
110  
111  
112  
113  
114  
115  
116  
117  
118  
119  
120  
121  
122  
123  
124  
125  
126  
127  
128  
129  
130  
131  
132  
133  
134  
135  
136  
137  
138  
139  
140  
141  
142  
143  
144  
145  
146  
147  
148  
149  
150  
151  
152  
153  
154  
155  
156  
157  
158  
159  
160  
161  
162  
163  
164  
165  
166  
167  
168  
169  
170  
171  
172  
173  
174  
175  
176  
177  
178  
179  
180  
181  
182  
183  
184  
185  
186  
187  
188  
189  
190  
191  
192  
193  
194  
195  
196  
197  
198  
199  
200  
201  
202  
203  
204  
205  
206  
207  
208  
209  
210  
211  
212  
213  
214  
215  
216  
217  
218  
219  
220  
221  
222  
223  
224  
225  
226  
227  
228  
229  
230  
231  
232  
233  
234  
235  
236  
237  
238  
239  
240  
241  
242  
243  
244  
245  
246  
247  
248  
249  
250  
251  
252  
253  
254  
255  
256  
257  
258  
259  
260  
261  
262  
263  
264  
265  
266  
267  
268  
269  
270  
271  
272  
273  
274  
275  
276  
277  
278  
279  
280  
281  
282  
283  
284  
285  
286  
287  
288  
289  
290  
291  
292  
293  
294  
295  
296  
297  
298  
299  
300  
301  
302  
303  
304  
305  
306  
307  
308  
309  
310  
311  
312  
313  
314  
315  
316  
317  
318  
319  
320  
321  
322  
323  
324  
325  
326  
327  
328  
329  
330  
331  
332  
333  
334  
335  
336  
337  
338  
339  
340  
341  
342  
343  
344  
345  
346  
347  
348  
349  
350  
351  
352  
353  
354  
355  
356  
357  
358  
359  
360  
361  
362  
363  
364  
365  
366  
367  
368  
369  
370  
371  
372  
373  
374  
375  
376  
377  
378  
379  
380  
381  
382  
383  
384  
385  
386  
387  
388  
389  
390  
391  
392  
393  
394  
395  
396  
397  
398  
399  
400  
401  
402  
403  
404  
405  
406  
407  
408  
409  
410  
411  
412  
413  
414  
415  
416  
417  
418  
419  
420  
421  
422  
423  
424  
425  
426  
427  
428  
429  
430  
431  
432  
433  
434  
435  
436  
437  
438  
439  
440  
441  
442  
443  
444  
445  
446  
447  
448  
449  
450  
451  
452  
453  
454  
455  
456  
457  
458  
459  
460  
461  
462  
463  
464  
465  
466  
467  
468  
469  
470  
471  
472  
473  
474  
475  
476  
477  
478  
479  
480  
481  
482  
483  
484  
485  
486  
487  
488  
489  
490  
491  
492  
493  
494  
495  
496  
497  
498  
499  
500  
501  
502  
503  
504  
505  
506  
507  
508  
509  
510  
511  
512  
513  
514  
515  
516  
517  
518  
519  
520  
521  
522  
523  
524  
525  
526  
527  
528  
529  
530  
531  
532  
533  
534  
535  
536  
537  
538  
539  
540  
541  
542  
543  
544  
545  
546  
547  
548  
549  
550  
551  
552  
553  
554  
555  
556  
557  
558  
559  
560  
561  
562  
563  
564  
565  
566  
567  
568  
569  
570  
571  
572  
573  
574  
575  
576  
577  
578  
579  
580  
581  
582  
583  
584  
585  
586  
587  
588  
589  
590  
591  
592  
593  
594  
595  
596  
597  
598  
599  
600  
601  
602  
603  
604  
605  
606  
607  
608  
609  
610  
611  
612  
613  
614  
615  
616  
617  
618  
619  
620  
621  
622  
623  
624  
625  
626  
627  
628  
629  
630  
631  
632  
633  
634  
635  
636  
637  
638  
639  
640  
641  
642  
643  
644  
645  
646  
647  
648  
649  
650  
651  
652  
653  
654  
655  
656  
657  
658  
659  
660  
661  
662  
663  
664  
665  
666  
667  
668  
669  
670  
671  
672  
673  
674  
675  
676  
677  
678  
679  
680  
681  
682  
683  
684  
685  
686  
687  
688  
689  
690  
691  
692  
693  
694  
695  
696  
697  
698  
699  
700  
701  
702  
703  
704  
705  
706  
707  
708  
709  
710  
711  
712  
713  
714  
715  
716  
717  
718  
719  
720  
721  
722  
723  
724  
725  
726  
727  
728  
729  
730  
731  
732  
733  
734  
735  
736  
737  
738  
739  
740  
741  
742  
743  
744  
745  
746  
747  
748  
749  
750  
751  
752  
753  
754  
755  
756  
757  
758  
759  
760  
761  
762  
763  
764  
765  
766  
767  
768  
769  
770  
771  
772  
773  
774  
775  
776  
777  
778  
779  
780  
781  
782  
783  
784  
785  
786  
787  
788  
789  
790  
791  
792  
793  
794  
795  
796  
797  
798  
799  
800  
801  
802  
803  
804  
805  
806  
807  
808  
809  
810  
811  
812  
813  
814  
815  
816  
817  
818  
819  
820  
821  
822  
823  
824  
825  
826  
827  
828  
829  
830  
831  
832  
833  
834  
835  
836  
837  
838  
839  
840  
841  
842  
843  
844  
845  
846  
847  
848  
849  
850  
851  
852  
853  
854  
855  
856  
857  
858  
859  
860  
861  
862  
863  
864  
865  
866  
867  
868  
869  
870  
871  
872  
873  
874  
875  
876  
877  
878  
879  
880  
881  
882  
883  
884  
885  
886  
887  
888  
889  
890  
891  
892  
893  
894  
895  
896  
897  
898  
899  
900  
901  
902  
903  
904  
905  
906  
907  
908  
909  
910  
911  
912  
913  
914  
915  
916  
917  
918  
919  
920  
921  
922  
923  
924  
925  
926  
927  
928  
929  
930  
931  
932  
933  
934  
935  
936  
937  
938  
939  
940  
941  
942  
943  
944  
945  
946  
947  
948  
949  
950  
951  
952  
953  
954  
955  
956  
957  
958  
959  
960  
961  
962  
963  
964  
965  
966  
967  
968  
969  
970  
971  
972  
973  
974  
975  
976  
977  
978  
979  
980  
981  
982  
983  
984  
985  
986  
987  
988  
989  
990  
991  
992  
993  
994  
995  
996  
997  
998  
999  
1000

10

58. The method of claim 57, further comprising:

step for processing the secret using the code;

wherein the step for unlocking the lock bit associated with the data stored in the first location comprises step for unlocking the lock bit associated with the data stored in the first location in response to the step for processing the secret using the code.

15

59. The method of claim 55, further comprising:

step for storing the secret within the first location securely;

20 step for storing data within the first location securely; and

step for storing code different from the secret and different from the data within the first location securely.

25 60. The method of claim 59, further comprising:

step for unlocking a lock bit associated with the data prior to the step for retrieving at least the portion of the data from the first location using the secret.

61. The method of claim 60, further comprising:

5 step for reading the code from the first location; and  
step for securing the code in a secure location different from the first location;  
wherein the step for retrieving at least the portion of the data from the first location using the  
secret comprises step for retrieving at least the portion of the data from the first  
location using the code and the secret.

62. The method of claim 55, further comprising:

step for reading the code from the first location; and  
step for securing the code in a secure location different from the first location;  
wherein the step for retrieving at least the portion of the data from the first location using the  
secret comprises step for retrieving at least a portion of the data from the first location  
using the code and the secret.

63. The method of claim 55, further comprising:

step for providing a lock bit associated with the data that when set provides an indication that  
the data stored in the first location is secured.

64. A method of securing data in a personal computer system, the method comprising:

step for storing a secret within a first location; and  
step for storing code different from the secret within the first location;

wherein the code is configured to provide access to data stored in the first location when processed in association with the secret.

65. The method of claim 64, further comprising:

5 step for providing a lock bit associated with the data stored in the first location that when step provides an indication that the data stored in the first location is secured.

66. A computer readable program storage device encoded with instructions that, when executed by a personal computer, performs a method of securely accessing data in the personal computer, the method comprising:

reading a secret from a first location;

securing the secret in a secure location different from the first location; and

retrieving at least a portion of the data stored in the first location using the secret.

67. The computer readable program storage device of claim 66, wherein the first location comprises a memory;

wherein reading the secret from the first location comprises reading the secret from the memory;

wherein securing the secret in the secure location different from the first location comprises

securing the secret in the secure location different from the memory; and

wherein retrieving at least the portion of the data stored in the first location using the secret comprises retrieving at least the portion of the data stored in the memory using the secret.

68. The computer readable program storage device of claim 67, wherein the memory is a read-only memory (ROM);

wherein reading a secret from the memory comprises reading the secret from the ROM;

wherein securing the secret in a secure location different from the memory comprises

5       securing the secret in the secure location different from the ROM; and

wherein retrieving at least a portion of the data stored in the memory using the secret comprises retrieving at least the portion of the data stored in the ROM using the secret.

10       69. The computer readable program storage device of claim 68, wherein the data comprises basic input-output system (BIOS) data and the ROM is a BIOS ROM configured to store the BIOS data;

wherein reading the secret from the ROM comprises reading the secret from the BIOS ROM;

wherein securing the secret in the secure location different from the ROM comprises securing

15       the secret in the secure location different from the BIOS ROM; and

wherein retrieving at least a portion of the data stored in the ROM using the secret comprises retrieving at least a portion of the BIOS data stored in the BIOS ROM using the secret.

20       70. The computer readable program storage device of claim 68, wherein reading the secret from the ROM comprises reading the secret from within the data stored within the ROM.

71. The computer readable program storage device of claim 66, the method further comprising:

25

reading code from the first location, wherein the code is different from the secret and  
different from the data stored in the first location;

wherein retrieving at least a portion of the data stored in the first location using the secret  
comprises retrieving at least a portion of the data stored in the first location using the  
code and the secret.

72. The computer readable program storage device of claim 71, wherein the first location  
comprises a memory;

wherein reading the secret from the first location comprises reading the secret from the  
memory;

wherein securing the secret in the secure location different from the first location comprises  
securing the secret in the secure location different from the memory;

wherein retrieving at least the portion of the data stored in the first location using the secret  
comprises retrieving at least the portion of the data stored in the memory using the  
secret;

wherein reading code from the first location comprises reading code from the memory  
wherein the code is different from the secret and different from the data stored in the  
memory; and

wherein retrieving at least the portion of the data stored in the first location using the code  
and the secret comprises retrieving at least a portion of the data stored in the memory  
using the code and the secret.

73. The computer readable program storage device of claim 72, wherein reading the secret within the memory and reading code from the memory further comprises reading the secret from inside the code within the memory.

5 74. The computer readable program storage device of claim 71, the method further comprising:

unlocking a lock bit associated with the data stored in the first location prior to retrieving at least the portion of the data stored in the first location using the secret.

10 75. The computer readable program storage device of claim 74, wherein the location comprises a memory;

wherein reading the secret from the first location comprises reading the secret from the memory;

15 wherein securing the secret in the secure location different from the first location comprises securing the secret in the secure location different from the memory;

wherein retrieving at least the portion of the data stored in the first location using the secret comprises retrieving at least the portion of the data stored in the memory using the secret;

wherein reading code from the first location comprises reading code from the memory

20 wherein the code is different from the secret and different from the data stored in the memory;

wherein retrieving at least the portion of the data stored in the first location using the code and the secret comprises retrieving at least a portion of the data stored in the memory using the code and the secret; and

wherein unlocking the lock bit associated with the data stored in the first location prior to  
retrieving at least the portion of the data stored in the first location using the secret  
comprises unlocking the lock bit associated with the data stored in the memory prior  
to retrieving at least the portion of the data stored in the memory using the secret.

5

76. The computer readable program storage device of claim 74, the method further  
comprising:

processing the secret using the code;

wherein unlocking a lock bit associated with the data stored in the first location comprises  
unlocking the lock bit associated with the data stored in the first location in response  
to processing the secret using the code.

10

77. The computer readable program storage device of claim 76, wherein the first location  
comprises a memory;

15

wherein reading the secret from the first location comprises reading the secret from the  
memory;

wherein securing the secret in the secure location different from the first location comprises  
securing the secret in the secure location different from the memory;

20 wherein retrieving at least the portion of the data stored in the first location using the secret  
comprises retrieving at least the portion of the data stored in the memory using the  
secret;

wherein reading code from the first location comprises reading code from the memory,  
wherein the code is different from the secret and different from the data stored in the  
memory;

25

wherein retrieving at least the portion of the data stored in the first location using the code  
and the secret comprises retrieving at least a portion of the data stored in the memory  
using the code and the secret;

wherein unlocking the lock bit associated with the data stored in the first location prior to  
5 retrieving at least the portion of the data stored in the first location using the secret  
comprises unlocking the lock bit associated with the data stored in the memory prior  
to retrieving at least the portion of the data stored in the memory using the secret; and

wherein unlocking the lock bit associated with the data stored in the first location comprises  
unlocking the lock bit associated with the data stored in the memory in response to  
10 processing the secret using the code.

78. The computer readable program storage device of claim 66, the method further  
comprising:

unlocking a lock bit associated with data stored in the first location prior to retrieving at least  
15 the portion of the data stored in the first location using the secret.

79. The computer readable program storage device of claim 78, wherein the first location  
comprises a memory;

wherein reading the secret from the first location comprises reading the secret from the  
20 memory;

wherein securing the secret in the secure location different from the first location comprises  
securing the secret in the secure location different from the memory;

wherein retrieving at least the portion of the data stored in the first location using the secret  
comprises retrieving at least the portion of the data stored in the memory using the  
25 secret; and



wherein unlocking a lock bit associated with data stored in the first location prior to retrieving at least the portion of the data stored in the first location using the secret comprises unlocking a lock bit associated with data stored in the memory prior to retrieving at least the portion of the data stored in the memory using the secret.

5

80. The computer readable program storage device of claim 66, further comprising:

storing the secret within the first location securely;

storing data within the first location securely; and

storing code different from the secret and different from the data within the first location securely.

10

81. The computer readable program storage device of claim 80, wherein the first location comprises a memory;

wherein reading the secret from the first location comprises reading the secret from the memory;

15

wherein securing the secret in the secure location different from the first location comprises securing the secret in the secure location different from the memory;

wherein retrieving at least the portion of the data stored in the first location using the secret comprises retrieving at least the portion of the data stored in the memory using the

20

secret;

wherein storing the secret within the first location securely comprises storing the secret within the memory securely;

wherein storing data within the first location securely comprises storing data within the memory securely; and

wherein storing code different from the secret and different from the data within the first location securely comprises storing code different from the secret and different from the data within the memory securely

- 5 82. The computer readable program storage device of claim 81, wherein the memory is a read-only memory (ROM);

wherein storing a secret within the memory comprises storing a secret within the ROM;

wherein storing data within the memory comprises storing data within the ROM;

wherein storing code different from the secret and different from the data within the memory  
10 comprises storing code different within secret and different from the data within the ROM;

wherein securing the secret in a secure location different from the memory comprises  
securing the secret in a secure location different from the ROM; and

wherein retrieving at least a portion of the data from the memory using the secret comprises  
15 retrieving at least a portion of the data from the ROM using the secret.

83. The computer readable program storage device of claim 82, wherein the data comprises basic input-output system (BIOS) data and the ROM is a BIOS ROM configured to store the BIOS data;

20 wherein storing a secret within the ROM comprises storing a secret within the BIOS ROM;  
wherein storing data within the ROM comprises storing data within the BIOS ROM;  
wherein storing code different within secret and different from the data within the ROM  
comprises storing code different within secret and different from the BIOS data within  
the BIOS ROM;

wherein securing the secret in a secure location different from the ROM comprises securing the secret in a secure location different from the BIOS ROM; and wherein retrieving at least a portion of the data from the ROM using the secret comprises retrieving at least a portion of the BIOS data from the BIOS ROM using the secret.

5

84. The computer readable program storage device of claim 81, wherein storing a secret within the memory and storing data within the memory comprises storing the secret inside the data within the memory.

85. The computer readable program storage device of claim 81, wherein storing a secret within the memory and storing code different from the secret and different from the data within the memory comprises storing the secret inside the code within the memory.

15 86. The computer readable program storage device of claim 81, further comprising: unlocking a lock bit associated with the data prior to retrieving at least the portion of the data from the memory using the secret.

87. The computer readable program storage device of claim 86, further comprising:

20 reading the code from the memory; and

securing the code in a secure location different from the memory;

wherein retrieving at least a portion of the data from the memory using the secret comprises retrieving at least a portion of the data from the memory using the code and the secret.

88. The computer readable program storage device of claim 87, wherein reading the secret from the memory comprises reading the secret from the memory during a boot sequence; and

wherein securing the secret in a secure location different from the memory comprises storing the secret in SMM memory space.

89. The computer readable program storage device of claim 87, wherein retrieving at least a portion of the data from the memory using the code and the secret further comprises:

processing the code; and

transmitting at least an indication of the secret to the memory;

90. The computer readable program storage device of claim 89, wherein retrieving at least a portion of the data from the memory using the code and the secret further comprises:

receiving a challenge from the memory; and

transmitting a response to the memory including at least an indication of the secret to the memory, in response to receiving the challenge.

91. The computer readable program storage device of claim 66, further comprising:

reading the code from the first location; and

securing the code in a secure location different from the first location;

wherein retrieving at least a portion of the data from the first location using the secret comprises retrieving at least a portion of the data from the first location using the code and the secret.

92. The computer readable program storage device of claim 91, wherein the first location comprises a memory;

wherein reading the secret from the first location comprises reading the secret from the  
5 memory;

wherein securing the secret in the secure location different from the first location comprises securing the secret in the secure location different from the memory;

wherein retrieving at least the portion of the data stored in the first location using the secret comprises retrieving at least the portion of the data stored in the memory using the  
10 secret;

wherein reading the code from the reading the code from the memory comprises reading the code from the memory;

wherein securing the code in a secure location different from the first location comprises securing the code in a secure location different from the memory; and

15 wherein retrieving at least a portion of the data from the first location using the secret further comprises retrieving at least a portion of the data from the memory using the code and the secret.

93. The computer readable program storage device of claim 66, wherein reading the  
20 secret from the first location comprises reading the secret from the first location during a boot sequence; and

wherein securing the secret in a secure location different from the first location comprises storing the secret in SMM memory space.

94. The computer readable program storage device of claim 93, wherein the first location comprises a memory;

wherein reading the secret from the first location comprises reading the secret from a memory;

5 wherein securing the secret in the secure location different from the first location comprises securing the secret in the secure location different from the memory;

wherein retrieving at least the portion of the data stored in the first location using the secret comprises retrieving at least the portion of the data stored in the memory using the secret; and

10 wherein reading the secret from the memory further comprises reading the secret from the memory during a boot sequence.

95. The computer readable program storage device of claim 66, further comprising:  
providing a lock bit associated with the data that when set provides an indication that the data  
15 stored in the memory is secured.

96. The computer readable program storage device of claim 95, wherein the first location comprises a memory;

20 wherein reading the secret from the first location comprises reading the secret from the memory;

wherein securing the secret in the secure location different from the first location comprises securing the secret in the secure location different from the memory;

25 wherein retrieving at least the portion of the data stored in the first location using the secret comprises retrieving at least the portion of the data stored in the memory using the secret; and

wherein providing the lock bit associated with the data that when set provides an indication that the data stored in the first location is secured comprises providing a lock bit associated with the data that when set provides an indication that the data stored in the memory is secured

5

97. A computer readable program storage device encoded with instructions that, when executed by a personal computer system, performs a method of securing data in the personal computer system, the method comprising:

storing a secret within a first location; and

10 storing code different from the secret within the first location;

wherein the code is configured to provide access to data stored in the first location when processed in association with the secret.

98. The computer readable program storage device of claim 97, wherein the first location comprises a memory;

15

wherein storing the secret within the first location comprises storing a secret within the memory;

wherein storing code different from the secret within the first location comprises storing code different from the secret within the memory; and

20 wherein the code is configured to provide access to data stored in the first location when processed in association with the secret further comprises the code being configured to provide access to data stored in the memory when processed in association with the secret.

99. The computer readable program storage device of claim 98, wherein the memory is a read-only memory (ROM);

wherein storing a secret within the memory comprises storing a secret within the ROM; and

wherein storing code different from the secret within the memory comprises storing code

5 different within secret within the ROM; and

wherein the code is configured to provide access to data stored in the ROM when processed in association with the secret.

100. The computer readable program storage device of claim 99, wherein the data comprises basic input-output system (BIOS) data and the ROM is a BIOS ROM configured to store the BIOS data;

wherein storing a secret within the ROM comprises storing a secret within the BIOS ROM;

wherein storing code different within secret within the ROM comprises storing code different within secret within the BIOS ROM; and

15 wherein the code is configured to provide access to BIOS data stored in the BIOS ROM when processed in association with the secret.

101. The computer readable program storage device of claim 98, wherein storing a secret within the memory comprises storing the secret inside the data within the memory.

102. The computer readable program storage device of claim 98, wherein storing a secret within the memory and storing code different from the secret within the memory comprises storing the secret inside the code within the memory.

103. The computer readable program storage device of claim 98, further comprising:



providing a lock bit associated with the data stored in the memory that when set provides an indication that the data stored in the memory is secured.

(b)  
 (c)  
 (d)  
 (e)  
 (f)  
 (g)  
 (h)  
 (i)  
 (j)  
 (k)  
 (l)  
 (m)  
 (n)  
 (o)  
 (p)  
 (q)  
 (r)  
 (s)  
 (t)  
 (u)  
 (v)  
 (w)  
 (x)  
 (y)  
 (z)